احمدرضا دانشور

کارشناس SOC سطح ۱

متولد: ۱۳۷۳/۳/۲۵

وضعیت تأهل: متأهل

وضعیت سربازی: پایان خدمت

ایمیل: daneshvar.ahmadreza@outlook.com

موبایل: (+۹۸)۹۱۷۶۷۱۲۴۲۸

آدرس: فارس، شیراز، شهرک جوادیه - خ محمد رسول الله ۳۴

هدف شغلی

تلاش دارم تا در نقش یک کارشناس امنیت، در سطح SOC Tier ۱ فعالیت کنم و به پیشگیری، شناسایی و پاسخ به تهدیدهای امنیتی در محیط‌های دیجیتالی کمک کنم. هدف من ارتقاء مهارت‌های امنیتی، یادگیری مداوم و توسعه دانش است تا بتوانم با استفاده از تکنولوژی‌های روز و ابزارهای متنوع، به ارتقاء امنیت و حفاظت از اطلاعات سازمان‌ها و سیاست‌ها بپردازم.

سوابق تحصیلی

کارشناسی برق

گرایش: قدرت

موسسه/دانشگاه: دانشگاه آزاد اسلامی واحد آباده آزاد

فارس، آباده

۱۳۹۴ - ۱۳۹۶

مهارت‌های کاربردی

- CoreLog SIEM
- آشنایی با Security Onion
- آشنایی با Sysmon
- آشنایی با Wireshark
- آشنایی با sguil
- آشنایی با Snort
- آشنایی با Suricata
- آشنایی با Zeek
- آشنایی با AppLocker
- آشنایی با Process Explorer
- کار با لینوکس(Ubuntu)
- آشنایی با Autoruns
- آشنایی با Mitre Attack فریمورک
- آشنایی با Nmap
- آشنایی با Metasploit
- آشنایی با Linux
- Microsoft Word
- Microsoft Excel
- طراحی سایت (CSS,HTML)

زبان

انگلیسی

مهارت خواندن آشنایی نسبی

مهارت نوشتن آشنایی نسبی

مهارت گفتاری مبتدی

مهارت شنیداری مبتدی

دوره‌ها و گواهینامه‌ها

- SOC Tier ۱

  موسسه: Ravin Academy

- SANS SEC۵۱۱.۳: Network Security Monitoring
- SANS SEC۵۱۱.۵: Continuous Security Monitoring
- Sans sec۵۰۳
- آشنایی با CoreLog SIEM
- OSCP
- Certified Ethical Hacker (C|EH)

  موسسه: Ravin Academy

- Security+

  موسسه: Douran Academy

- Network+

  موسسه: Arjang Academy

- Using Mitre Att&ck For Cyber Intelligence
- آشنایی سطحی با مفاهیم CCNA و MCSA
- آشنایی با مفاهیم آسیب پذیری های تحت وب
- Introduction to Network Analysis
- آموزش تحلیل بدافزار مقدماتی

  موسسه: مکتب خونه

تجربیات

- حل لابراتور های SANS ۵۱۱
- کار با ابزارهای تحلیل شبکه

علاقه‌مندی‌ها

- مطالعه کتب امنیت سایبری
- شرکت در رویدادها و کنفرانس‌های امنیت
- پیگیری تکنولوژی‌های جدید

اهداف

اهداف کوتاه مدت

برطرف کردن نیازهای امنیتی سازمان به صورت کامل، شناسایی ضعف‌ها و مشکلات امنیتی و ارائه راهکارهای جلوگیری از آنها.

اهداف بلند مدت

۱. تقویت توانایی‌های امنیتی شخصی از طریق حضور در دوره‌ها و آموزش‌های پیشرفته.
۲. شناخت عمیق‌تر از تهدیدها و روش‌های مقابله با آنها با تحلیل دقیق‌تر رویدادهای امنیتی.
۳. پیشرفت در حوزه مدیریت امنیت و همکاری با تیم‌های امنیتی برای بهبود فرآیندها و پاسخگویی به تهدیدها.

درباره من

یک کارشناس امنیت سایبری تازه‌کار هستم که با علاقه به یادگیری مداوم و توسعه مهارت‌های امنیتی، به دنبال ارتقاء امنیت و حفاظت از اطلاعات سازمان‌ها و شبکه‌ها می‌باشم.

سوابق شغلی

Soc Analyst

سازمان فاوا شهرداری شیراز

فارس، شیراز

بهمن ۱۴۰۲ - اکنون

وظایف و دستاوردها

- بهبود قوانین سامانه SIEM
- تحقیق و بررسی رویداد ها
- پیگیری و تحلیل رویدادهای امنیتی و شناسایی تهدیدهای احتمالی
- تدوین گزارش‌های دوره‌ای از وضعیت امنیت شبکه و پیشنهاد تدابیر بهبودی
- شرکت در جلسات تیم بررسی حوادث امنیتی و ارائه راهکارهای اصلاحی
- پیگیری نصب و پیکربندی تجهیزات امنیتی مانند فایروال و آنتی‌ویروس در سازمان

تحقیقات

DNS Exfilteration